БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к магистерской диссертации

СБОР ИНФОРМАЦИИ О ДОСТУПЕ К СЕРВЕРУ С ЦЕЛЬЮ АНАЛИЗА УРОВНЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Ещенко Павел Витальевич

Научный руководитель — доктор физико-математических наук,
профессор В. М. Котов

2015

Реферат

Магистерская диссертация, 47 страниц, 7 рисунков, 9 таблиц, 12 источников.

АНАЛИЗАТОР ЛОГ-ФАЙЛОВ, СБОРЩИКИ ЛОГФАЙЛОВ, ХРАНЕНИЕ, ВЫБОРКА, БЕЗОПАСНОСТЬ, ИНДЕКСАЦИЯ, ГРАФИЧЕСКОЕ ОТОБРАЖЕНИЕ, СКРИПТ, КОНФИГУРИРОВАНИЕ

Объект исследования — программные продукты с открытым исходным кодом, позволяющие построить систему безопасности.

Предмет исследования – возможность построения системы безопасности на программных продуктах с открытым исходным кодом.

Цель работы – разработка системы предотвращения атак веб-сервисов.

Результат – построение системы безопасности, позволяющей в режиме реального времени предоставлять в графическом виде уровень различных типов атак, происходящих в данный момент, а также возможность их отражать. Система основана на продуктах с открытым исходным кодом.

Структура магистерской диссертации представлена 2 главами. В первой главе сначала рассматривается возможность построение системы безопасности на основе лог-файлов, а затем дается краткий обзор анализаторов лог-файлов а также их сравнение. Во второй главе описываются и рассматриваются используемые программные продукты, их установка и настройка, описание построения инфраструктуры для анализа лог файлов, а также скрипты взаимодействия между ними.

Автор магистерской диссертации подтверждает, что работа выполнена самостоятельно и приведенный в ней расчетно-аналитический материал правильно и объективно отражает состояние исследуемого процесса, а все заимствованные из литературных и других источников теоретические, методологические положения и концепции сопровождаются ссылками на их авторов.

Abstract

Master thesis, 47 pages, 7 figures, 9 tables, 12 references.

GENERAL DESCRIPTION OF THE WORK Keywords: LOG ANALYZER, LOG FILE COLLECTORS, STORAGE, SAMPLING, SAFETY, INDEXING, GRAPHICAL DISPLAY, SCRIPT CONFIGURATION.

Objective –to develop a system to prevent attacks web services.

The task of preventing attacks are an integral and important part of the functioning of the web services.

The object of study is open source software that allows to build a security system.

The subject of research is the possibility of building security system on products with open source software.

Significant results include: the construction of the security system that allows real time providing a graphic level of the various types of attacks occurring at the moment, and the ability to reflect them. Importantly, the system is based on products with open source software.

The structure of the Master's thesis presented two heads. The first chapter discusses the possibility of construction of the security system based on log files. A brief review of the log file analyzers as well as their comparison. In the second chapter describes and addresses used by software, its installation and configuration, description of construction of the infrastructure for the analysis of log files and scripts interaction between them.

The author of the work confirms that the work is done independently, computational and analytical information correctly and objectively reflects the state of subject and all borrowed from literature and other sources of theoretical, methodological principles, and concepts are accompanied by references to their authors.